Math 361

February 27, 2023

Tomorrow's quiz

See posting at our homepage.

Today

Catch-up.

- Finish proving basic results about the Noetherian property from last week.
- Prove the Hilbert basis theorem.

Noetherian modules

Definition. An R-module M is *Noetherian* if every submodule of M is finitely generated.

Noetherian modules

Definition. An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

Noetherian modules

Definition. An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

1. M is Noetherian.

Noetherian modules

Definition. An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

1. M is Noetherian.
2. M satisfies the ascending chain condition on submodules:

Noetherian modules

Definition. An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

1. M is Noetherian.
2. M satisfies the ascending chain condition on submodules: every chain of submodules of M,
$$N_1 \subseteq N_2 \subseteq \cdots ,$$
eventually *stabilizes*.

Noetherian modules

Definition. An R-module M is *Noetherian* if every submodule of M is finitely generated.

Proposition. The following are equivalent for an R-module M:

1. M is Noetherian.
2. M satisfies the ascending chain condition on submodules: every chain of submodules of M,
$$N_1 \subseteq N_2 \subseteq \cdots ,$$
eventually *stabilizes*.
3. Every nonempty collection of submodules of M has a maximal element under inclusion.

Mappings of R-modules

A sequence of R-module mappings

$$M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$$

is *exact at* M if $\operatorname{im}\phi = \ker\psi$.

Mappings of R-modules

A sequence of R-module mappings

$$M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$$

is *exact at M* if $\operatorname{im}\phi = \ker\psi$.

Examples.

$0 \to M' \xrightarrow{\phi} M$ is exact at M' if and only if ϕ is injective.

Mappings of R-modules

A sequence of R-module mappings

$$M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$$

is *exact at* M if $\operatorname{im} \phi = \ker \psi$.

Examples.

$0 \to M' \xrightarrow{\phi} M$ is exact at M' if and only if ϕ is injective.

$M \xrightarrow{\psi} M'' \to 0$ is exact at M'' if and only if ψ is surjective.

Mappings of R-modules

A sequence of R-module mappings

$$M' \xrightarrow{\phi} M \xrightarrow{\psi} M''$$

is *exact at M* if $\operatorname{im} \phi = \ker \psi$.

Examples.

$0 \to M' \xrightarrow{\phi} M$ is exact at M' if and only if ϕ is injective.

$M \xrightarrow{\psi} M'' \to 0$ is exact at M'' if and only if ψ is surjective.

If the s.e.s.

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

is exact, then $M/\operatorname{im}(\phi) \xrightarrow{\sim} M''$.

Noetherian property and mappings of R-modules

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules.

Noetherian property and mappings of R-modules

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Noetherian property and mappings of R-modules

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Corollary. If R is a Noetherian ring, then so is R^n for all $n \in \mathbb{N}$.

Noetherian property and mappings of R-modules

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Corollary. If R is a Noetherian ring, then so is R^n for all $n \in \mathbb{N}$.

Proof. If $n = 0, 1$, the result is trivial.

Noetherian property and mappings of R-modules

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Corollary. If R is a Noetherian ring, then so is R^n for all $n \in \mathbb{N}$.

Proof. If $n = 0, 1$, the result is trivial. Let $n > 1$, and suppose the statement is true for R^k with $0 \leq k < n$.

Noetherian property and mappings of R-modules

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Corollary. If R is a Noetherian ring, then so is R^n for all $n \in \mathbb{N}$.

Proof. If $n = 0, 1$, the result is trivial. Let $n > 1$, and suppose the statement is true for R^k with $0 \leq k < n$.

We have the short exact sequence

$$0 \to R \xrightarrow{\psi} R^n \xrightarrow{\phi} R^{n-1} \to 0.$$

where $\psi(r) = (r, 0, \ldots, 0)$ and $\phi(r_1, \ldots, r_n) = (r_2, \ldots, r_n)$.

Noetherian property and mappings of R-modules

Proposition. Let

$$0 \to M' \xrightarrow{\phi} M \xrightarrow{\psi} M'' \to 0$$

be a short exact sequence of R-modules. Then M is Noetherian if and only if M' and M'' are Noetherian.

Corollary. If R is a Noetherian ring, then so is R^n for all $n \in \mathbb{N}$.

Proof. If $n = 0, 1$, the result is trivial. Let $n > 1$, and suppose the statement is true for R^k with $0 \leq k < n$.

We have the short exact sequence

$$0 \to R \xrightarrow{\psi} R^n \xrightarrow{\phi} R^{n-1} \to 0.$$

where $\psi(r) = (r, 0, \ldots, 0)$ and $\phi(r_1, \ldots, r_n) = (r_2, \ldots, r_n)$.

The result now follows by induction and the proposition we just proved. $\square$

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module.

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated.

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. $(\Rightarrow)$

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. ($\Rightarrow$) Duh.

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. $(\Rightarrow)$ Duh. $(\Leftarrow)$ Now suppose that M is finitely generated.

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. ($\Rightarrow$) Duh. ($\Leftarrow$) Now suppose that M is finitely generated. Say $M = \mathrm{Span}_R\{m_1, \ldots, m_n\}$.

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. ($\Rightarrow$) Duh. ($\Leftarrow$) Now suppose that M is finitely generated. Say $M = \mathrm{Span}_R\{m_1, \ldots, m_n\}$. We then have a surjective homomorphism

$$\psi\colon R^n \to M$$

$$(r_1, \ldots, r_n) \mapsto \sum_{i=1}^n r_i m_i.$$

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. ($\Rightarrow$) Duh. ($\Leftarrow$) Now suppose that M is finitely generated. Say $M = \mathrm{Span}_R\{m_1, \ldots, m_n\}$. We then have a surjective homomorphism

$$\psi \colon R^n \to M$$
$$(r_1, \ldots, r_n) \mapsto \sum_{i=1}^{n} r_i m_i.$$

We have a short exact sequence: $0 \to \ker(\psi) \to R^n \xrightarrow{\psi} M \to 0$.

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. ($\Rightarrow$) Duh. ($\Leftarrow$) Now suppose that M is finitely generated. Say $M = \mathrm{Span}_R\{m_1, \ldots, m_n\}$. We then have a surjective homomorphism

$$\psi\colon R^n \to M$$
$$(r_1, \ldots, r_n) \mapsto \sum_{i=1}^{n} r_i m_i.$$

We have a short exact sequence: $0 \to \ker(\psi) \to R^n \xrightarrow{\psi} M \to 0$.

Then R Noetherian $\Rightarrow$

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. ($\Rightarrow$) Duh. ($\Leftarrow$) Now suppose that M is finitely generated. Say $M = \mathrm{Span}_R\{m_1, \ldots, m_n\}$. We then have a surjective homomorphism

$$\psi \colon R^n \to M$$
$$(r_1, \ldots, r_n) \mapsto \sum_{i=1}^{n} r_i m_i.$$

We have a short exact sequence: $0 \to \ker(\psi) \to R^n \xrightarrow{\psi} M \to 0$.

Then R Noetherian $\Rightarrow$ R^n Noetherian

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. ($\Rightarrow$) Duh. ($\Leftarrow$) Now suppose that M is finitely generated. Say $M = \mathrm{Span}_R\{m_1, \ldots, m_n\}$. We then have a surjective homomorphism

$$\psi \colon R^n \to M$$

$$(r_1, \ldots, r_n) \mapsto \sum_{i=1}^{n} r_i m_i.$$

We have a short exact sequence: $0 \to \ker(\psi) \to R^n \xrightarrow{\psi} M \to 0$.

Then R Noetherian $\Rightarrow$ R^n Noetherian $\Rightarrow$

Noetherian property and mappings of R-modules

Corollary. If R is Noetherian and M is an R-module. Then M is Noetherian if and only if M is finitely generated. In other words, a finitely generated module over a Noetherian ring is Noetherian.

Proof. ($\Rightarrow$) Duh. ($\Leftarrow$) Now suppose that M is finitely generated. Say $M = \mathrm{Span}_R\{m_1, \ldots, m_n\}$. We then have a surjective homomorphism

$$\psi \colon R^n \to M$$
$$(r_1, \ldots, r_n) \mapsto \sum_{i=1}^{n} r_i m_i.$$

We have a short exact sequence: $0 \to \ker(\psi) \to R^n \xrightarrow{\psi} M \to 0$.

Then R Noetherian $\Rightarrow$ R^n Noetherian $\Rightarrow$ M Noetherian. $\square$

Noetherian property and mappings of R-modules

Corollary. Let K be a number field. Then its ring of integer $\mathfrak{O}_K$ is Noetherian.

Noetherian property and mappings of R-modules

Corollary. Let K be a number field. Then its ring of integer $\mathfrak{O}_K$ is Noetherian.

Proof. This follows since $\mathbb{Z}$ is a PID, hence, Noetherian, and $\mathfrak{O}_K$ is a finitely generated $\mathbb{Z}$-module. $\square$

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$. Suppose not.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$. Suppose not. Let (x) be a maximal element of $\mathcal{A}$ (why possible?).

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$. Suppose not. Let (x) be a maximal element of $\mathcal{A}$ (why possible?). Is x irreducible?

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$. Suppose not. Let (x) be a maximal element of $\mathcal{A}$ (why possible?). Is x irreducible? No.

So $x = yz$ with y, z non-units.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$. Suppose not. Let (x) be a maximal element of $\mathcal{A}$ (why possible?). Is x irreducible? No.

So $x = yz$ with y, z non-units. We have $(x) \subsetneq (y)$ and $(x) \subsetneq (z)$. (See blackboard.)

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$. Suppose not. Let (x) be a maximal element of $\mathcal{A}$ (why possible?). Is x irreducible? No.

So $x = yz$ with y, z non-units. We have $(x) \subsetneq (y)$ and $(x) \subsetneq (z)$. (See blackboard.) By maximality of (x), we have $(y), (z) \notin \mathcal{A}$.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$. Suppose not. Let (x) be a maximal element of $\mathcal{A}$ (why possible?). Is x irreducible? No.

So $x = yz$ with y, z non-units. We have $(x) \subsetneq (y)$ and $(x) \subsetneq (z)$. (See blackboard.) By maximality of (x), we have $(y), (z) \notin \mathcal{A}$. So y and z factor into irreducibles.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$. Suppose not. Let (x) be a maximal element of $\mathcal{A}$ (why possible?). Is x irreducible? No.

So $x = yz$ with y, z non-units. We have $(x) \subsetneq (y)$ and $(x) \subsetneq (z)$. (See blackboard.) By maximality of (x), we have $(y), (z) \notin \mathcal{A}$. So y and z factor into irreducibles. But then x factors into irreducibles since $x = yz$.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero non-unit element of R can be factored into irreducibles.

Proof. Let $\mathcal{A}$ be the set of principal ideals $(x) \subseteq R$ such that $x \neq 0$, x is a non-unit, and x cannot be factored into irreducibles.

Goal: show $\mathcal{A} = \emptyset$. Suppose not. Let (x) be a maximal element of $\mathcal{A}$ (why possible?). Is x irreducible? No.

So $x = yz$ with y, z non-units. We have $(x) \subsetneq (y)$ and $(x) \subsetneq (z)$. (See blackboard.) By maximality of (x), we have $(y), (z) \notin \mathcal{A}$. So y and z factor into irreducibles. But then x factors into irreducibles since $x = yz$. Contradiction. $\square$

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero element of R can be factored into irreducibles.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero element of R can be factored into irreducibles.

Corollary. Let K be a number field. Then every element of its ring of integers, $\mathfrak{O}_K$, can be factored into irreducibles in $\mathfrak{O}_K$.

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero element of R can be factored into irreducibles.

Corollary. Let K be a number field. Then every element of its ring of integers, $\mathfrak{O}_K$, can be factored into irreducibles in $\mathfrak{O}_K$.

Proof. We have seen that $\mathfrak{O}_K$ is finitely generated over the Noetherian ring $\mathbb{Z}$. $\square$

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero element of R can be factored into irreducibles.

Corollary. Let K be a number field. Then every element of its ring of integers, $\mathfrak{O}_K$, can be factored into irreducibles in $\mathfrak{O}_K$.

Proof. We have seen that $\mathfrak{O}_K$ is finitely generated over the Noetherian ring $\mathbb{Z}$. $\square$

In homework, we've seen that $\mathbb{Q}(\sqrt{-5})$ is not a UFD:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Factorization in Noetherian domains

Theorem. Let R be a Noetherian domain. Then every nonzero element of R can be factored into irreducibles.

Corollary. Let K be a number field. Then every element of its ring of integers, $\mathfrak{O}_K$, can be factored into irreducibles in $\mathfrak{O}_K$.

Proof. We have seen that $\mathfrak{O}_K$ is finitely generated over the Noetherian ring $\mathbb{Z}$. $\square$

In homework, we've seen that $\mathbb{Q}(\sqrt{-5})$ is not a UFD:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Does this contradict the Corollary?

Hilbert basis theorem

Hilbert basis theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Hilbert basis theorem

Hilbert basis theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remarks.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \ldots, s_n \in S$ such that $S = \{f(s_1, \ldots, s_n) : f \in R[x_1, \ldots, x_n]\}$.

Hilbert basis theorem

Hilbert basis theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remarks.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \ldots, s_n \in S$ such that $S = \{f(s_1, \ldots, s_n) : f \in R[x_1, \ldots, x_n]\}$.

  Example: $R[x_1, \ldots, x_n]$ is finitely generated as a ring over R but not as a module over R.

Hilbert basis theorem

Hilbert basis theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remarks.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \ldots, s_n \in S$ such that $S = \{f(s_1, \ldots, s_n) : f \in R[x_1, \ldots, x_n]\}$.

  Example: $R[x_1, \ldots, x_n]$ is finitely generated as a ring over R but not as a module over R.
- Recall that a ring R is Noetherian, if and only if all of its ideals are finitely generated.

Hilbert basis theorem

Hilbert basis theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remarks.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \ldots, s_n \in S$ such that $S = \{f(s_1, \ldots, s_n) : f \in R[x_1, \ldots, x_n]\}$.

  Example: $R[x_1, \ldots, x_n]$ is finitely generated as a ring over R but not as a module over R.
- Recall that a ring R is Noetherian, if and only if all of its ideals are finitely generated.
- Letting $R = K$ be a field and $S = K[x_1, \ldots, x_n]$, the Hilbert basis theorem says

Hilbert basis theorem

Hilbert basis theorem. Let R and S be rings with $R \subseteq S$. Suppose that S is finitely generated as a ring over R and R is Noetherian. Then S is a Noetherian ring.

Remarks.

- For S to be *finitely generated as a ring* over R, we mean that there exist $s_1, \ldots, s_n \in S$ such that $S = \{f(s_1, \ldots, s_n) : f \in R[x_1, \ldots, x_n]\}$.

  Example: $R[x_1, \ldots, x_n]$ is finitely generated as a ring over R but not as a module over R.
- Recall that a ring R is Noetherian, if and only if all of its ideals are finitely generated.
- Letting $R = K$ be a field and $S = K[x_1, \ldots, x_n]$, the Hilbert basis theorem says that every ideal in S finitely generated.

Proof of Hilbert basis theorem

Suppose that $s_1, \ldots, s_n$ generate S as a ring over R.

Proof of Hilbert basis theorem

Suppose that $s_1, \ldots, s_n$ generate S as a ring over R.

We need to show that S is Noetherian.

Proof of Hilbert basis theorem

Suppose that $s_1, \ldots, s_n$ generate S as a ring over R.

We need to show that S is Noetherian. Then there exists an R-module surjection

$$\begin{aligned} R[x_1, \ldots, x_n] &\to S \\ f(x_1, \ldots, x_n) &\mapsto f(s_1, \ldots, s_n). \end{aligned}$$

Proof of Hilbert basis theorem

Suppose that $s_1, \ldots, s_n$ generate S as a ring over R.

We need to show that S is Noetherian. Then there exists an R-module surjection

$$\begin{aligned} R[x_1, \ldots, x_n] &\to S \\ f(x_1, \ldots, x_n) &\mapsto f(s_1, \ldots, s_n). \end{aligned}$$

Since the image of a Noetherian R-module is Noetherian, it suffices to prove that the polynomial ring $R[x_1, \ldots, x_n]$ is a Noetherian R-module.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

Note that $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

Note that $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$. For instance,

$$\mathbb{Z}[x, y] \ni xy^3 + 5xy^2 + 7x^5y^3 + 9x^6y^2 + 15 =$$

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

Note that $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$. For instance,

$$\begin{aligned}\mathbb{Z}[x, y] \ni xy^3 + 5xy^2 + 7x^5y^3 + 9x^6y^2 + 15 = \\ (x + 7x^5)y^3 + (5x + 9x^6)y^2 + 15 \in \mathbb{Z}[x][y].\end{aligned}$$

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x_1, \ldots, x_n]$ Noetherian.

We do this by induction on n. The base case is $n = 0$, which is just R, itself, which is Noetherian.

Note that $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$. For instance,

$$\mathbb{Z}[x, y] \ni xy^3 + 5xy^2 + 7x^5y^3 + 9x^6y^2 + 15 = \\ (x + 7x^5)y^3 + (5x + 9x^6)y^2 + 15 \in \mathbb{Z}[x][y].$$

By induction, it suffices to show that R Noetherian $\Rightarrow R[x]$ Noetherian.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow$ $R[x]$ Noetherian.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow$ $R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow$ $R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

We must show that

$$I = (f_1, \ldots, f_k)$$

for some $f_1, \ldots, f_k \in I$.

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

We must show that

$$I = (f_1, \ldots, f_k)$$

for some $f_1, \ldots, f_k \in I$.

What is wrong with the following argument?

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

We must show that

$$I = (f_1, \ldots, f_k)$$

for some $f_1, \ldots, f_k \in I$.

What is wrong with the following argument? In fact, $I = (f)$ for some f since $R[x]$ is a PID (from the division algorithm).

Proof of the Hilbert basis theorem

To show: R Noetherian $\Rightarrow R[x]$ Noetherian.

Let $I \subseteq R[x]$ be an ideal.

We must show that

$$I = (f_1, \ldots, f_k)$$

for some $f_1, \ldots, f_k \in I$.

What is wrong with the following argument? In fact, $I = (f)$ for some f since $R[x]$ is a PID (from the division algorithm).

Answer: The division algorithm assumes R is a field.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$,

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$,

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Finally, given a, as above, and $r \in R$,

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Finally, given a, as above, and $r \in R$, we have $rf \in I$

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Finally, given a, as above, and $r \in R$, we have $rf \in I$ so its leading term, ra, is in A.

Proof of the Hilbert basis theorem

If $f = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$ with $a_d \neq 0$, then call a_d the *leading coefficient* of f. (For completeness, say the zero polynomial has leading coefficient 0.)

Let $A \subseteq R$ be the set of leading coefficients of elements of I.

Is A and ideal of R?

Claim. A is an ideal of R.

Proof. First, $0 \in A$, so $A \neq \emptyset$. Next suppose $a, b \in A$. Say they are leading coefficients of f, g, respectively. Without loss of generality $\deg(f) \leq \deg(g)$. Let $d = \deg(g) - \deg(f)$. Then $x^d f + g \in I$, so its leading coefficient, $a + b$ is in A. So A is closed under addition.

Finally, given a, as above, and $r \in R$, we have $rf \in I$ so its leading term, ra, is in A. Hence, A is closed under "outside-in" multiplication. $\square$

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I \subseteq R[x].$$

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I \subseteq R[x].$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I \subseteq R[x].$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module,

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \dots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I \subseteq R[x].$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \dots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module, M is Noetherian.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I \subseteq R[x].$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module, M is Noetherian. Hence, $I_{<d}$ is a finitely generated R-module.

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I \subseteq R[x].$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module, M is Noetherian. Hence, $I_{<d}$ is a finitely generated R-module. Say

$$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\}.$$

Proof of the Hilbert basis theorem

Let $A \subseteq R$ be the ideal of leading coefficients of elements of I.

Since R is Noetherian, $A = (a_1, \ldots, a_s)$ for some s. Pick $g_i \in R[x]$ with leading coefficient a_i for each i.

Scaling by appropriate powers of x, we may assume all g_i have the same degree d. Define

$$I_{<d} = \{f \in I : \deg(f) < d\} \subseteq I \subseteq R[x].$$

Then $I_{<d}$ is an R-submodule of $M := \mathrm{Span}_R\{1, x, x^2, \ldots, x^{d-1}\}$.

Since R is Noetherian, and M is a finitely generated R-module, M is Noetherian. Hence, $I_{<d}$ is a finitely generated R-module. Say

$$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\}.$$

Claim: $I = (g_1, \ldots, g_s, h_1, \ldots, h_t)$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\}$ = all elements of I of degree $< d$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\}$ = all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\}$ = all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$,

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be a

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Then $f - \sum_{i=1}^{s} r_i x^{e-d} g_i \in I$,

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Then $f - \sum_{i=1}^{s} r_i x^{e-d} g_i \in I$, and has degree $< e$.

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Then $f - \sum_{i=1}^{s} r_i x^{e-d} g_i \in I$, and has degree $< e$.

We are done by induction on the degree of f. (Why?)

Proof of the Hilbert basis theorem

$A = (a_1, \ldots, a_s) \subseteq R$, ideal of leading coeffs. of elements of I.

$g_1, \ldots, g_s \in I$ polys of degree d with leading coeffs. $a_1, \ldots, a_s$.

$I_{<d} = \mathrm{Span}_R\{h_1, \ldots, h_t\} =$ all elements of I of degree $< d$.

Claim: $I = (g_1, \ldots, g_s, \ldots, h_1, \ldots, h_s)$.

Proof. Let $f \in I$. If $\deg(f) < d$, no problem. (Why?)

Suppose $\deg(f) = e \geq d$, and let the leading coefficient of f be $a \in A$. We have $a = \sum_{i=1}^{s} r_i a_i$ for some $r_i \in R$.

Then $f - \sum_{i=1}^{s} r_i x^{e-d} g_i \in I$, and has degree $< e$.

We are done by induction on the degree of f. (Why?) $\square$